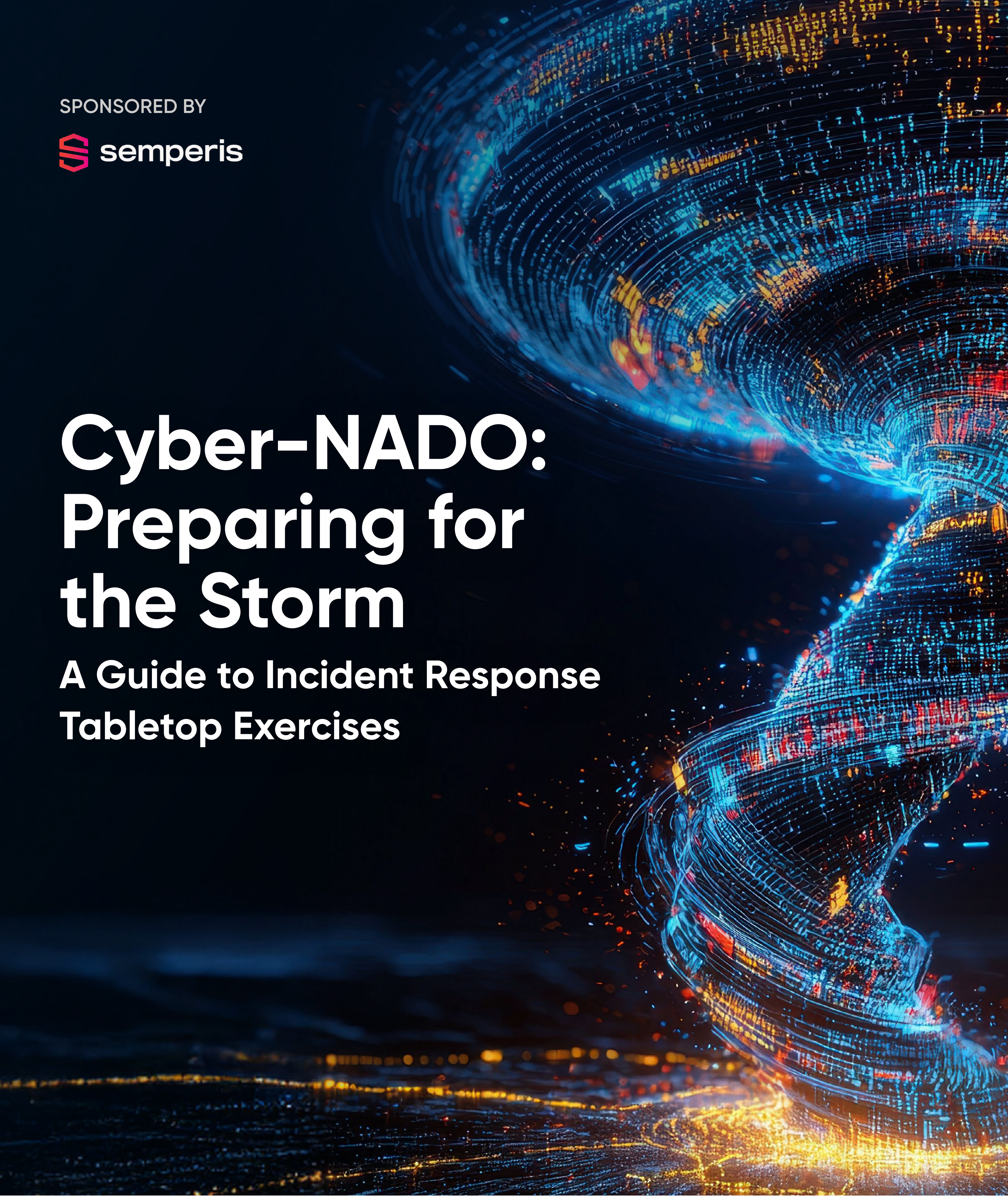


SPONSORED BY

semperis

Cyber-NADO: Preparing for the Storm

A Guide to Incident Response Tabletop Exercises

SC Media

CyberRisk Collaborative

CRA | Business Intelligence

SC CISO Stories

INTRODUCTION

The Calm Before the Storm

Imagine standing on a quiet beach as dark clouds begin to form on the horizon. The wind picks up, the air turns heavy, and before you know it, a full-blown hurricane is upon you. Cyber incidents are much like these storms; unpredictable, chaotic, and capable of causing widespread devastation in a matter of minutes. The difference between surviving the disaster and suffering irreversible damage is preparation. Just as communities conduct emergency drills for natural disasters, organizations must practice their response to cyber threats before they strike.

Cyberattacks are no longer a question of "if" but "when," making proactive preparation an essential part of any organization's security strategy. Despite having detailed Incident Response Plans (IRPs) in place, many businesses fail to test them regularly, leaving teams unprepared when a real breach occurs. This guide focuses on the power of Incident Response Tabletop Exercises (TTX), structured simulations that allow organizations to evaluate their response plans, identify weaknesses, and enhance coordination among key stakeholders. By walking through realistic cyberattack scenarios, teams can refine their decision-making, improve collaboration, and ensure they respond effectively when faced with a real crisis.

This guide will provide a step-by-step approach to running a successful tabletop exercise, from assembling the right team to conducting and analyzing the session for continuous improvement. Whether you are a security leader, IT professional, or executive decision-maker, this resource will help you build a resilient cyber defense strategy. Cyber incidents can feel like a relentless storm, but with proper preparation, your organization can weather the chaos and emerge stronger. By the end of this guide, you will be equipped with the tools and knowledge to conduct impactful tabletop exercises, strengthen your response capabilities, and ensure your organization is ready for the next cyber-NADO.

Who Should Read This?

CISOs & Security Leaders
To assess response readiness

IT & Security Teams
To refine technical defenses

Executives & Risk Managers
To align business strategy with cybersecurity

Legal & Compliance Teams
To ensure regulatory and legal preparedness

Understanding the Cyber-NADO

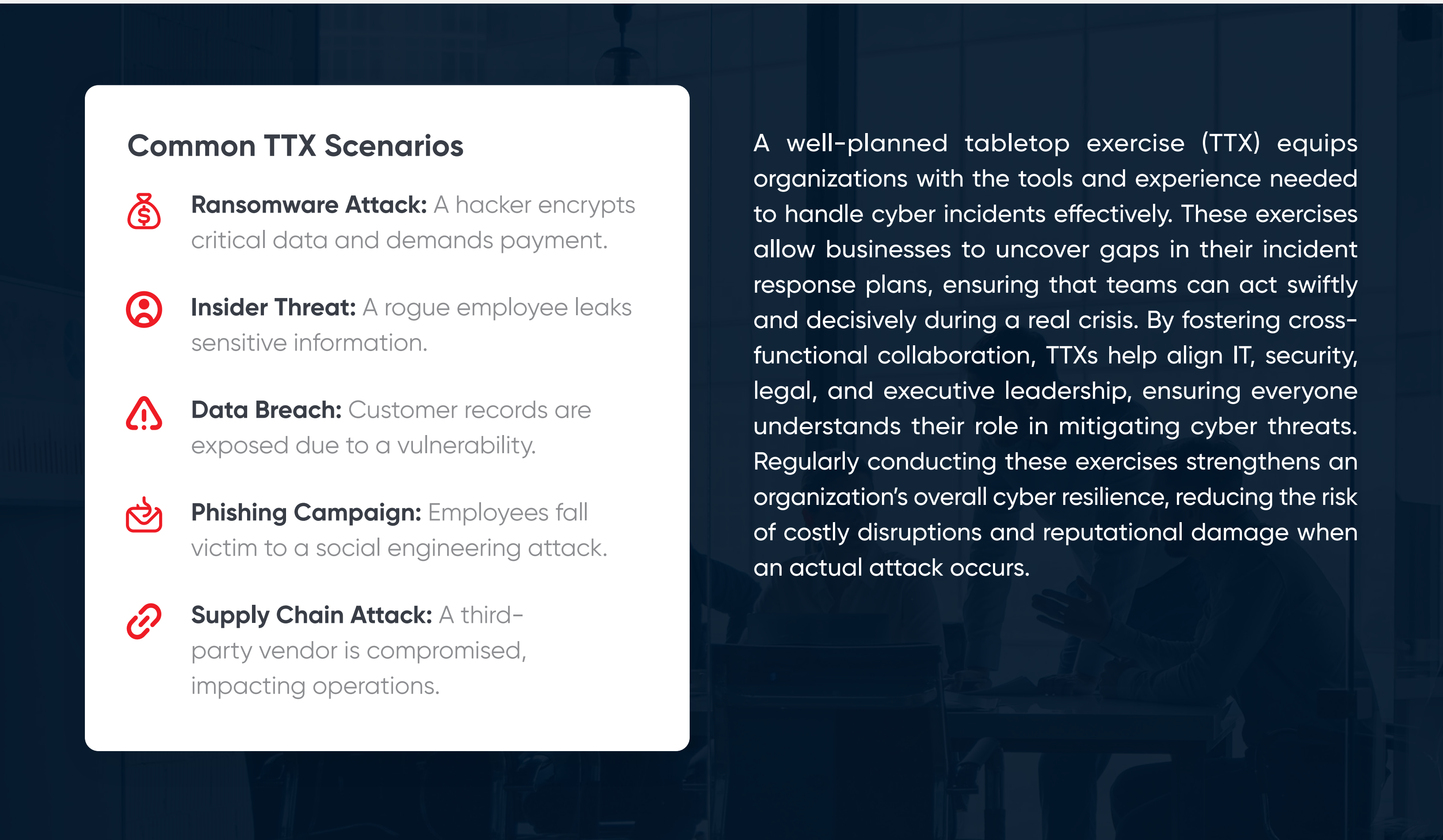
What Are Tabletop Exercises?

A Tabletop Exercise (TTX) is a structured, discussion-based activity designed to simulate a cyber incident and test an organization's response capabilities. Unlike live penetration tests or red team engagements, which focus on technical defenses and actively attempting to breach a network, a TTX emphasizes decision-making, coordination, and strategic response. These exercises are typically conducted in a conference room or virtual setting, where key stakeholders walk through a realistic cyber threat scenario step by step. The goal is not to test individual technical skills but to evaluate how well the incident response team works together, identifies threats, and makes critical decisions under pressure.

Why Tabletop Exercises Matter

Many organizations have an **Incident Response Plan (IRP)**, but how often is it tested? TTX helps teams:

- Identify **gaps** in existing response plans.
- Improve **cross-functional coordination** between IT, legal, PR, and executives.
- Reduce **reaction time** during a real incident.
- Ensure compliance with **industry regulations** like NIST, ISO 27001, and GDPR.



Common TTX Scenarios

- **Ransomware Attack:** A hacker encrypts critical data and demands payment.
- **Insider Threat:** A rogue employee leaks sensitive information.
- **Data Breach:** Customer records are exposed due to a vulnerability.
- **Phishing Campaign:** Employees fall victim to a social engineering attack.
- **Supply Chain Attack:** A third-party vendor is compromised, impacting operations.

A well-planned tabletop exercise (TTX) equips organizations with the tools and experience needed to handle cyber incidents effectively. These exercises allow businesses to uncover gaps in their incident response plans, ensuring that teams can act swiftly and decisively during a real crisis. By fostering cross-functional collaboration, TTXs help align IT, security, legal, and executive leadership, ensuring everyone understands their role in mitigating cyber threats. Regularly conducting these exercises strengthens an organization's overall cyber resilience, reducing the risk of costly disruptions and reputational damage when an actual attack occurs.

Assembling the Response Team

Who's at the Table?

CYBER INCIDENTS ARE NOT JUST AN IT PROBLEM. It requires a collaborative effort across multiple teams. The effectiveness of a TTX depends on having the right people in the room.

Key Players in a Tabletop Exercise

IT & Security Team

These professionals analyze system logs, assess vulnerabilities, and implement technical measures to stop the threat from spreading. They also coordinate with external cybersecurity partners, such as forensic investigators or law enforcement, to determine the root cause and prevent future incidents.

Legal & Compliance Team

This team ensures the organization meets regulatory requirements and avoids legal repercussions after a security breach. In addition, they help determine if and when the organization must disclose the breach to authorities, customers, or other stakeholders while minimizing liability.

Executive Leadership

Senior leaders and decision-makers provide strategic direction during an incident response. Executives also decide on high-stakes issues, such as whether to pay a ransom in a ransomware attack or how to manage customer relationships in the aftermath of a data breach.

Human Resources (HR)

They help enforce policies, coordinate with legal teams on disciplinary actions, and provide guidance on employee privacy rights. HR also ensures that internal messaging related to the incident is handled appropriately, avoiding unnecessary panic or misinformation among staff.

PR & Communications Team

This team is responsible for crafting clear, accurate, and timely messages to employees, customers, the media, and stakeholders. They work closely with legal teams to ensure that public statements align with compliance requirements while maintaining transparency and trust. Their goal is to control the narrative, preventing misinformation from escalating the crisis.

Roles and Responsibilities

- **Incident Commander**: Leads response efforts.
- **Technical Leads**: Investigate the incident and execute containment.
- **Legal Advisor**: Ensures compliance with breach notification laws.
- **Communications Lead**: Manages public and internal messaging.

Conducting the Tabletop Exercise

The Cyber-NADO Strikes

Now that the team is assembled, it's time to **run the exercise**. A well-executed TTX follows a structured approach to maximize learning and engagement.

Step-by-Step Guide to Running a Tabletop Exercise

1 Define Objectives

- Are you testing **technical response or executive decision-making**?
- Do you want to **validate compliance** with regulatory requirements?
- Are you assessing **internal vs. external communication strategies**?

2 Choose the Scenario

Pick a realistic cyber threat that aligns with your industry. For example:

- A **healthcare organization** might focus on ransomware targeting patient records.
- A **financial institution** might simulate a phishing attack leading to fraud.

3 Prepare the Exercise

- Assign roles and distribute briefing materials.
- Keep the scenario **engaging** but **realistic**.
- Ensure **all key stakeholders** are present.

4 Facilitate the Discussion

- Present the scenario and let participants **walk through their response**.
- Introduce **unexpected twists** (e.g., media leak, regulatory intervention) to simulate real-life challenges.
- Encourage open discussion- **what worked? what didn't?**

5 Capture Lessons Learned

- Document key insights and action items.
- Identify **gaps** in processes, policies, or technology.

Common Challenges & How to Overcome Them

Participants are too passive

↳ Use role-playing to drive engagement.

Scenario is unrealistic

↳ Tailor it to industry-specific threats.

Lack of follow-up actions

↳ Assign ownership for improvements.

After the Storm

Improving Your Incident Response Plan

The true value of a TTX lies in the **post-exercise analysis**. Without proper follow-up, the exercise is just another meeting.

Debriefing & Reviewing the Exercise

- Hold a **post-mortem discussion** immediately after the exercise.
- Capture **key takeaways, strengths, and weaknesses**.
- Assign **action items** to address identified gaps.

Updating & Strengthening the Incident Response Plan (IRP)

- **Refine response playbooks** based on TTX findings.
- **Address gaps** in personnel, tools, or processes.
- **Update communication templates** for legal, PR, and customer notifications.

How Often Should You Conduct TTX?

- **Quarterly**: If you operate in a high-risk industry.
- **Biannually**: To maintain preparedness.
- **Annually**: At a minimum, to ensure your IRP remains effective.

Final Thoughts

The Next Cyber-nado is Coming

Just like natural disasters, cyber threats are inevitable—it's not a question of if an attack will happen, but when. The digital landscape is constantly evolving, with new vulnerabilities, sophisticated ransomware, and emerging attack vectors threatening organizations across every industry. Businesses that fail to proactively prepare risk not only financial losses but also reputational damage, legal repercussions, and operational disruption. However, those that take a strategic approach—by testing their response plans, training their teams, and refining their incident management processes—will be the ones that weather the storm successfully.

A strong incident response strategy is not built overnight; it requires continuous testing, improvement, and collaboration across multiple departments. Tabletop exercises (TTX) provide organizations with a safe, controlled environment to simulate cyberattacks, identify weaknesses, and strengthen response coordination before a real crisis occurs. By integrating IT, security, legal, PR, and executive leadership into these exercises, businesses ensure that everyone understands their role in mitigating threats and making critical decisions under pressure. The lessons learned from a well-executed TTX can be the difference between a swift recovery and total chaos when a real cyber incident occurs.

Don't wait until your organization is in the middle of a cyber-NADO to discover that your response plan is ineffective. Take action now by implementing regular tabletop exercises, refining your incident response procedures, and ensuring your team is prepared to detect, contain, and mitigate cyber threats efficiently. The next cyberstorm is coming, will your organization be ready?

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and now LaunchTech Communications.
To learn more, visit CyberRiskAlliance.com.

SPONSORED BY

As cybersecurity leaders and Active Directory (AD) experts, we know that identity-first security is the key to operational resilience. For more than 90% of today's enterprise organizations, if AD isn't secure, nothing is. Many of the world's leading businesses trust Semperis to help them protect AD and Azure AD from escalating cyber threats. Nothing is off-limits to today's cyberattackers, including emergency services, hospitals and healthcare providers, schools, and financial institutions. Whether your business is building businesses, saving lives, or serving citizens, we help you operate with confidence by protecting your critical identity infrastructure. To learn more, visit semperis.com.

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com